

**REMARKS**

Applicant thanks the Examiner for the careful consideration given to this application and for the helpful interview conducted on January 19, 2010 (summarized below). Reconsideration is now respectfully requested in view of the following remarks.

Claims 1, 2, and 4-18 are pending in this application. Claims 1, 5, 14, and 18 are independent claims. Reconsideration and allowance of the present application are respectfully requested.

**Entry of Amendment After Final Rejection**

Entry of the Amendment is requested under 37 C.F.R. § 1.116 because the Amendment: a) places the application in condition for allowance for the reasons discussed herein; b) does not present any additional claims without canceling the corresponding number of final rejected claims; and/or c) places the application in better form for an appeal, if an appeal is necessary. Entry of the Amendment is thus respectfully requested.

**Summary of Interview of January 19, 2010**

Applicants again thank the Examiner for the (telephonic) interview conducted on January 19, 2010. The interview was conducted between Examiner Shewaye Gelagay and Applicants' undersigned representative. During the interview, the application of the references to Inada et al. and Colligan et al. were discussed, *vis a vis* the claimed "manager terminal." With respect to Inada et al., the Examiner stressed that col. 5 of Inada et al. discusses that the apparatus described may receive a "management packet." However, the undersigned pointed out that there is no indication from where such a management packet is received. The Examiner's position was that it is implicit that a management packet is received from some kind of management terminal. With respect to Colligan et al., the undersigned pointed out that the cited portions (i.e., in the Office Action) all refer to operations performed within a VOD apparatus. However, during the discussion, it was noted that other portions of Colligan et al. may discuss decryption and re-encryption by distribution servers. However, no teaching of distribution of a "time period

for encryption” was explicitly found in Colligan et al. The Examiner suggested that the claims may be amended to more explicitly recite the “manager terminal.” No agreement was reached.

### **Claim Rejections Under 35 U.S.C. § 103**

Claims 1-2, 4-9 and 12-18 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,604,807 to Yamaguchi et al. (hereinafter “Yamaguchi et al.”) in view of “Transparent Network Security Policy Enforcement,” USENIX 2000 (hereinafter “Keromytis et al.”) and in view of U.S. Patent No. 6,775,769 to Inada et al. (hereinafter “Inada et al.”) and in view of U.S. Patent No. 6,415,031 to Colligan et al. (hereinafter “Colligan et al.”). This rejection is respectfully traversed for at least the following reasons.

Independent Claim 1 includes recitation of “a manager terminal to input information into the encryption apparatus and into each of the plurality of communications terminals having encrypting capability, the information including an indication of whether or not data packets are to be discarded between specific communication terminals after the data packets have been received and a time period for encryption.” Independent Claim 5 includes recitation of “a manager terminal to input information, including at least information for instructing whether or not data packets are to be discarded between specific communications terminals after the data packets have been received and a time period for encryption, into the encryption apparatus and those of the plurality of communications terminals having encryption capabilities, thereby completing a setting of each of the apparatus and communications terminals having encryption capabilities for communicating encrypted data.” Independent Claim 14 includes recitation of “information including whether or not data packets are to be discarded between specific communications terminals after the data packets have been received and a time period for the encryption are inputted from a manager terminal into each of the encryption apparatus and those of the plurality of communications terminals having the encrypting capability.” Finally, independent Claim 18 includes recitation of “a manager terminal for inputting information including an indication of whether or not data packets are to be discarded between specific communications terminals after the data packets have been received, and including a time period for encryption into each of the encryption apparatuses.” Applicants maintain that the cited

references fail to teach or suggest all of the details of these claim elements for at least the following reasons.

The Office Action, noting page 4, acknowledges that “[Yamaguchi et al. and Keromytis et al.] do not explicitly disclose information including whether or not data packets are to be discarded between specific terminals after the data packets have been received.” However, the Office Action then alleges that “Inada [et al.] in analogous art, however, discloses information including whether or not data packets are to be discarded between specific terminals after the data packets have been received (col. 5, line 25 – col. 6, line 65; col. 15, line 25 – col. 16, line 56; col. 17, lines 24-63).” Applicants respectfully disagree.’

The cited portions of Inada et al. at cols. 5-6 describe “the function block configuration of a cryptographic apparatus,” shown in Fig. 1. Col. 5, lines 16-17. During the interview, the Examiner pointed to col. 5, lines 23-31, which describe terminal function block 1 of Fig. 1, and which includes the discussion of “a management packet for managing the repeater-type cryptographic apparatus.” Col. 5, lines 27-28. The remainder of this part of the cited portion includes discussion of “plaintext output filter 25,” “ciphertext output filter 23,” and “home station output filter 24.” The discussions describe how these filters will discard “discard information.” However, there is no nexus between the “management packet” and any information regarding the discarding of information/packets. That is, at least this portion of Inada et al. fails to teach that the cryptographic apparatus receives from a manager terminal “information for instructing whether or not data packets are to be discarded between specific communications terminals after the data packets have been received,” as claimed.

Moving to col. 15, line 25 – col. 16, line 56, this portion of Inada et al. also provides description of a “home station input filter 31” and a “plaintext input filter 32” (with reference to Fig. 11). Again, there is no indication that “information for instructing whether or not data packets are to be discarded between specific communications terminals after the data packets have been received” is provided to these filters.

Finally, col. 17, lines 24-63 appear to merely provide a summary of what was previously presented in Inada et al. They, too, fail to indicate the provision of “information for instructing whether or not data packets are to be discarded between specific communications terminals after the data packets have been received.”

The Office Action, noting page 5, further states, “None of the references explicitly disclose input information including a time period for encryption.” The Office Action then alleges, “Colligan [et al.] in analogous art, however, discloses inputting information including a time period for encryption. (col. 8, line 7-18; col. 8, line 65 – col. 9, line 5).” Applicants respectfully disagree.

Applicants note that the cited portions of Colligan et al., at cols. 8-9, refer to the encryption of information in a video-on-demand (VOD) source 402 (see, e.g., col. 7, lines 60 ff.) and discuss scheduling of encryption and the use of an encryption key based on “an appropriate time epoch.” Col. 9, lines 25-26. Applicants also note the discussion of cols. 5-7 of Colligan et al., during the above-summarized interview. These portions of Colligan et al. refer to the furnishing of encrypted information to a remote server 404 and how it may be decrypted and then re-encrypted at the video server. However, nowhere is there any discussion of providing “a time period for encryption,” as claimed, to the server. On the contrary, Colligan et al. discusses, e.g., at col. 5, lines 29-37, “Subsequently, when the remote server (404) receives (508) a request for transmission of the video program from a subscriber station (110), the remote server (404) responds by first decrypting (510) the video program from the first encrypted form. A first key is may be [sic] used to accomplish such decryption (510), and such key may have been received from the video on-demand source (402) via a communication channel that is separate from the one used to transmit the video program.” See, also, col. 6, lines 13-24 and lines 57-64, and col. 7, lines 13-19. In all of these cases, there is no time period information transmitted to the server (or to any other component) in Inada et al.; on the contrary, the key necessary for decryption is provided, and therefore, there is no need to provide such “a time period for encryption.”

Furthermore, Applicants respectfully submit that none of the other cited references cure the deficiencies noted above.

Therefore, Applicants respectfully request that this rejection of Claims 1-2, 4-9 and 12-18 under 35 U.S.C. § 103 be withdrawn.

Claims 10-11 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Yamaguchi et al., in view of Keromytis et al. and in view of Inada et al. and in view of Colligan

et al., and in view of U.S. Patent No. 5,481,610 to Doiron et al. (hereinafter “Doiron et al.”). This rejection is respectfully traversed.

Claims 10 and 11 depend from Claim 1 and thus incorporate all of the elements of Claim 1. As noted above, the references cited in connection with the rejection of Claim 1 fail to teach or suggest all of the elements of Claim 1. Applicants submit that Doiron et al. fails to address the deficiencies of the other cited references and, therefore, that Claims 10 and 11 are allowable for at least the reasons discussed above.

Therefore, Applicants respectfully request that this rejection of Claims 10-11 under 35 U.S.C. § 103 be withdrawn.

**Disclaimer**

Applicants may not have presented all possible arguments or have refuted the characterizations of either the claims or the prior art as found in the Office Action. However, the lack of such arguments or refutations is not intended to act as a waiver of such arguments or as concurrence with such characterizations.

**CONCLUSION**

In view of the above, consideration and allowance are respectfully solicited.

In the event the Examiner believes an interview might serve in any way to advance the prosecution of this application, the undersigned is available at the telephone number noted below.

The Office is authorized to charge any necessary fees to Deposit Account No. 22-0185.

Applicant believes no fee is due with this response. However, if a fee is due, please charge our Deposit Account No. 22-0185, under Order No. 27592-01101-US1 from which the undersigned is authorized to draw.

Dated: February 12, 2010

Respectfully submitted,

Electronic signature: /Jeffrey W. Gluck/  
Jeffrey W. Gluck  
Registration No.: 44,457  
CONNOLLY BOVE LODGE & HUTZ LLP  
1875 Eye Street, NW  
Suite 1100  
Washington, DC 20006  
(202) 331-7111  
(202) 572-0322 (Direct Dial)  
(202) 293-6229 (Fax)  
Attorney for Applicant